JB

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-313341

(43)Date of publication of application : 24.11.1998

(51)Int.Cl. H04L 12/56
G06F 13/00
H04L 12/24
H04L 12/26
H04L 29/14

(21)Application number : 10-058104

(22)Date of filing : 10.03.1998

(71)Applicant : NATL AEROSPACE LAB
KAGAKU GIJUTSU SHINKO JIGYODAN

(72)Inventor : FUJITA NAOYUKI

(30)Priority

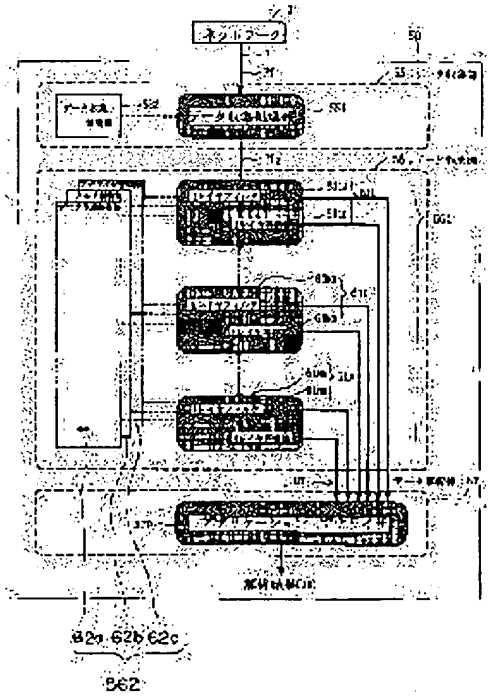
Priority number : 09 56715 Priority date : 11.03.1997 Priority country : JP

(54) METHOD FOR ANALYZING ILLEGAL COMMUNICATION ON NETWORK, SYSTEM FOR ANALYZING ILLEGAL COMMUNICATION ON NETWORK USING THE METHOD, AND RECORDING MEDIUM READABLE BY COMPUTER RECORDING NETWORK ILLEGAL COMMUNICATION ANALYSIS PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable a system to handle optional data, to handle optional communication between networks, to facilitate coping with the increase in number of protocols and to handle arbitrary protocols.

SOLUTION: This network illegal communication analysis system 50 analyzes illegal communication on a network, where communication is conducted between information communication stations according to a hierarchical protocol. The system 50 consists of a data collection section 55 that receives a packet PT transmitted on the network 3, a data generating section 56 that sets a parameter of a hierarchical module in response to the hierarchical protocol, based on information in a configuration file read in advance and processes a packet from the data collection section with each hierarchical module to generate analysis data DT, and a data analysis section 57 that discriminates the response of illegal commutation in the analysis data DT, based on the content described on the file.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－313341

(43)公開日　平成10年(1998)11月24日

(51)Int.Cl.[6]		識別記号	FI		
H04L	12/56		H04L	11/20	102Z
G06F	13/00	351	G06F	13/00	351Z
H04L	12/24		H04L	11/08	
	12/26			13/00	313
	29/14				

審査請求　有　請求項の数3　ＯＬ（全 15 頁）

(21)出願番号　特願平10－58104

(22)出願日　平成10年(1998)３月10日

(31)優先権主張番号　特願平9－56715

(32)優先日　平９(1997)３月11日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　391037397
科学技術庁航空宇宙技術研究所長
東京都調布市深大寺東町７丁目44番地１

(71)出願人　396020800
科学技術振興事業団
埼玉県川口市本町４丁目１番８号

(72)発明者　藤田　直行
東京都小金井市前原町４－17－28

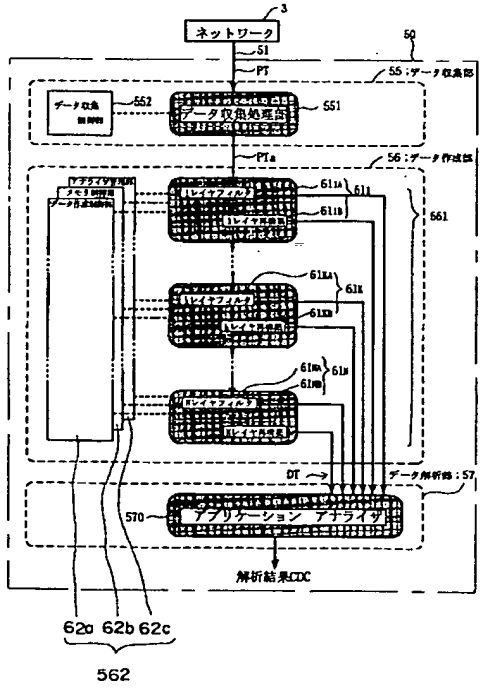
(74)代理人　弁理士　村瀬　一美

(54)【発明の名称】　ネットワーク不正解析方法及びこれを利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】　任意のデータを取り扱え、ネットワーク間の任意の通信を扱えて、プロトコル数の増大に容易に対処でき、任意のプロトコルを取り扱うことができるようにする。

【解決手段】　ネットワーク不正解析システム５０は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うネットワークでの不正を解析するものである。このシステム５０は、ネットワーク３上で伝送されているパケットＰＴを取り込むデータ収集部５５と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルでの情報に基づいて設定し、データ収集部からのパケットを各階層化モジュールで処理し解析データＤＴを作成するデータ作成部５６と、同ファイルに記載された内容を基に解析データＤＴに不正発生の有無を判定するデータ解析部５７とからなる。



【特許請求の範囲】

【請求項１】　情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する方法であって、前記ネットワーク上で伝送されているパケットを取り込むデータ収集工程と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、前記データ収集工程からのパケットを前記各階層化モジュールでフィルタリングして前記パケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基に前記データ作成工程からの解析データに不正が発生しているか判定するデータ解析工程とを備えたことを特徴とするネットワーク不正解析方法。

【請求項２】　情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する装置であって、前記ネットワーク上で伝送されているパケットを取り込むデータ収集部と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、前記データ収集部からのパケットを前記各階層化モジュールでフィルタリングして前記パケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成部と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基に前記データ作成部からの解析データに不正が発生しているか判定するデータ解析部とを備えたことを特徴とするネットワーク不正解析装置。

【請求項３】　情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、前記データ収集手順からのパケットを前記各階層化モジュールでフィルタリングして前記パケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基に前記データ作成手順からの解析データに不正が発生しているか判定するデータ解析手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワーク不正解析方法及びこれを利用した装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。さらに詳述すると、本発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおいて通信されるデータに不正が発生しているか否かを解析しネットワークのセキュリティやネットワーク管理を実行できるネットワーク不正解析方法及びこれを利用した装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【０００２】本明細書中では、ネットワークにおける「不正」とは例えばクラッキング等のいわゆる不正アクセスを意味する。

【０００３】

【従来の技術】従来、情報ステーションの間でデータの交換を行うように構成されたシステムにおいて、交換されるデータに不正が発生しているか否かを解析する解析方法が種々提供されている。

【０００４】まず、上記解析方法の第１の従来技術としては、例えば７層モデルのトランスポート層（トランスポートレイヤ）上に位置して動作し、トランスポートレイヤから通信内容を受け取り、オペレーティングシステムが用意している関数により、発信元をチェックし予め登録してある許可されるべき発信元かどうかの判定をするようにした解析システムが提案されている（ＴＣＰ ＷＲＡＰＰＥＲ；Mar19 1996 ）。

【０００５】また、上記解析方法の第２の従来技術としては、ネットワーク通信の機能を使用しないソフトウエアであって、所定の圧縮方法を用いて膨大なハードディスクの内容を圧縮しておき、定期的に保存してある内容と現在の圧縮した内容が一致するか否か比較することによりハードディスクへの不正なアクセスを検知するものがある（The Design and Implementation of Tripwire ; Feb 23 1995 ）。

【０００６】さらに、上記解析方法の第３の従来技術としては、典型的な不正（クラッキング（Cracking））手法が格納されていて、その手法を解析対象のシステムに対して実行することにより、当該システムの不正をチェックするようにしたものがある（Satan-network security scanner）。

【０００７】また、上記解析方法の第４の従来技術としては、ネットワーク通信そのものより、ネットワーク通信によってクラッキングされてしまう設定になっていないかどうかをホストコンピュータ毎に解析するものであって、ホストコンピュータのさまざまな設定内容がセキュリティ的に危険なものでないかオペレーティングシステムのコマンドを用いてチェックを行うようにしたものがある（COPS;Nov 171991）。

【０００８】上記解析方法の第５の従来技術としては、ＵＮＩＸで用いられているユーザのパスワードが妥当なものであるかどうかをチェックするものであって、パス

ワードの候補ファイルをもっていて候補の単語を暗号化し、暗号化した結果作成された暗号化された単語と暗号化されているパスワードとを比較し、一致すればいま暗号化した単語がパスワードであることを利用してパスワードの検索をおこなうようにしたシステムがある（Crack Version 4.1 ；Mar 3 1992 ）。

【０００９】上記解析方法の第６の従来技術としては、物理層パケット単位の解析を行うものがある（Sniffer ）。

【００１０】さらに、上記解析方法の第７の従来技術としては、階層化されたプロトコルにより情報ステーション間の通信を行うネットワークの診断システムであって、下位のレイヤフィルタから提供されたサービスデータユニットを入力制御からの解析指示に従って解析するとともに、上位のレイヤフィルタに対するサービスデータユニットを作成して提供するようにしたものがある（特開平４－３１５３４３号公報）。

【００１１】

【発明が解決しようとする課題】しかしながら、上記第１の従来技術によれば、トランスポートレイヤからデータを受け取るのみで、他のレイヤからデータを受けるものではないため、解析するデータが少なく不正の解析に十分ではない欠点がある。また、オペレーティングシステムの機能によりデータの再構築を行っているので、不正の解析に十分ではないという欠点がある。

【００１２】上記第２の従来技術によれば、ネットワーク通信機能を有していないため、ネットワーク通信のデータの不正解析ができないという欠点があった。

【００１３】さらに、これら第１，２の従来技術によれば、監視対象ホストコンピュータやホストステーション（以下、単に「ホスト」という）毎に当該解析方法を実現するプログラムをインストールする設計となっているため、ホスト数の増大に対応できない。

【００１４】そして、上記第３～５の従来技術によれば、解析プロトコル毎に新たな解析を行う設計となっているため、プロトコル数の増大に対応できない。

【００１５】また、上記第６の従来技術によれば、物理層パケット単位の解析を行う設計となっているため、クラッキング解析に不可欠なアプリケーション層セッション単位の解析ができない。

【００１６】一方、上記第７の従来技術によれば、プロトコルの各レイヤ毎に同一モジュールで当該レイヤ部分のデータのフィルタリングと診断とをおこなうようになっているため、他のレイヤとの関連で不正を解析することができず、不正の解析が十分とはいえないという欠点があった。

【００１７】そこで、本発明の第１の目的は、アプリケーションのセッションを含め任意のデータを取り扱うことができるネットワーク不正解析方法及びこの方法を利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【００１８】また、本発明の第２の目的は、ネットワーク間の任意の通信を扱うとともに、プロトコル数の増大に容易に対処できるネットワーク不正解析方法及びこの方法を利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【００１９】さらに、本発明の第３の目的は、任意のプロトコルを取り扱うことができるネットワーク不正解析方法及びこの方法を利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【００２０】

【課題を解決するための手段】上記第１～第３の目的を達成するため、請求項１記載の発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するネットワーク不正解析方法であって、ネットワーク上で伝送されているパケットを取り込むデータ収集工程と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成工程からの解析データに不正が発生しているか判定するデータ解析工程とを備えるようにしている。

【００２１】したがって、データ作成工程において、データ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成しているので、データ解析工程ではデータとして意味のある再構築後の解析データが解析対象となる。このため、データ部分に発生した不正を容易に判別することができる。

【００２２】特にネットワークにおける不正はデータ部分に発生することが多いので、このデータ部分の解析を行うことが有効であるが、ネットワーク上で伝送されているパケットではデータ部分が細分化されているので、このデータ部分に不正が発生したかを判定するのは困難である。これに対し、本発明では再構築後の意味のあるデータを解析対象としているのでデータ部分に不正が発生したかを容易に判定することができる。

【００２３】また、請求項２記載の発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するネットワーク不正解析装置装置であって、ネットワ

ーク上で伝送されているパケットを取り込むデータ収集部と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集部からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成部と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部からの解析データに不正が発生しているか判定するデータ解析部とを備えるようにしている。

【００２４】したがって、データ作成部において、データ収集部からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成しているので、データ解析部ではデータとして意味のある再構築後の解析データが解析対象となる。このため、データ部分に発生した不正を容易に判別することができる。

【００２５】さらに、請求項３記載の発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成手順からの解析データに不正が発生しているか判定するデータ解析手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体としている。

【００２６】したがって、コンピュータで記録媒体に格納されたプログラムを読み取り、インストールすることによってあるいはそのままプログラムを実行することによって、ネットワーク伝送時にデータ部分に発生した不正を容易に判別することができる。

【００２７】

【発明の実施の形態】以下、本発明の構成を図面に示す実施の形態の一例に基づいて詳細に説明する。図２に、本発明に係るネットワーク不正解析方法が適用されたネットワークシステムの一例を示す。

【００２８】この図２において、符号１は構内ネットワーク（以下、「ＬＡＮ」という）であり、このＬＡＮ１にはルータ２を介して緩衝帯ネットワーク３が接続されている。この緩衝帯ネットワーク３は、ルータ６を介して外部ネットワーク７に接続されている。

【００２９】本実施形態ではＬＡＮ１は、複数のステーション（図示せず）と、これらステーションを結ぶネットワーク（図示せず）と、外部に接続する外部接続回線１１とからなる。この外部接続回線１１はルータ２に接続されている。但し、ＬＡＮ１としては上述のものに限られず、単一のステーションから成るものとすることもできる。

【００３０】緩衝帯ネットワーク３は、本発明に係るネットワーク不正解析方法を実現するネットワーク不正解析システム５０と、コモンバス５１と、外部接続回線５２、５３とからなる。ネットワーク不正解析システム５０はコモンバス５１に接続されている。外部接続回線５２はルータ２とコモンバス５１とを接続している。外部接続回線５３はコモンバス５１とルータ６とを接続している。

【００３１】また、ネットワーク不正解析システム５０は従来のネットワーク不正解析システムと同様にコンピュータシステムにて構成される。このコンピュータシステムは、特に図示していないが、例えば各種の演算処理を実行する中央演算処理装置と、演算処理を実行する上で必要なプログラムやデータ等を記憶する主記憶装置と、入出力ポート等の各種インタフェースと、このネットワーク不正解析システムを実現するプログラムやその処理を実行する上で必要な各種データや定数等を記憶する例えばハードディスクドライブ装置と、データや必要な指令を入力する入力装置と、中央演算処理装置で処理した結果を出力する出力装置とから構成されるのが一般的である。

【００３２】図３に、本発明に係るネットワーク不正解析方法の実施の一形態を示す。この図３において、ネットワーク不正解析システム５０は、中央演算処理装置が主記憶装置に記憶されたプログラムを処理することにより実現されるものであって、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するシステムである。すなわち、ネットワーク不正解析システム５０は、例えば緩衝帯ネットワーク３で伝送されているパケットＰＴを取り込むデータ収集工程を実行するデータ収集部５５と、データ収集部５５からのパケットＰＴａを各階層化モジュールでフィルタリング及び再構築することにより解析データＤＴを作成するデータ作成工程を実行するデータ作成部５６と、データ作成部５６からの解析データＤＴに不正が発生しているか判定して解析結果ＣＤＣを出力するデータ解析工程を実行するデータ解析部５７とから構成されている。

【００３３】図１に、ネットワーク不正解析システム５０の詳細構成を示す。この図１において、データ収集部５５は、例えば緩衝帯ネットワーク３の間で伝送されているパケットＰＴを取り込むデータ収集処理部５５１と、このデータ収集処理部５５１のデータ収集処理を制御するデータ収集制御部５５２とから構成されている。データ収集処理部５５１は、収集したパケットＰＴをデ

ータ作成部５６に供給する。

【００３４】データ作成部５６は、階層化されたプロトコルに応じた階層化モジュールのパラメータを、予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集部５５からのパケットＰＴａを各階層化モジュールでフィルタリングしてパケットＰＴａの細分化されたデータを元の単位に再構築することにより解析データＤＴを作成するデータ作成工程を実行するものである。

【００３５】このデータ作成部５６は、大別すると、階層化モジュール５６１と、これを制御し管理する制御管理部５６２とから構成されている。制御管理部５６２は、予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて、階層化されたプロトコルに応じた階層化モジュール５６１のパラメータを設定できる。また、階層化モジュール５６１は、設定に基づいてデータ収集部５５からのパケットＰＴａをフィルタリングしてパケットＰＴａの細分化されたデータを元の単位に再構築することにより解析データＤＴを作成できるようになっている。

【００３６】階層化モジュール５６１は、１レイヤモジュール61_1，…，ｋレイヤモジュール61_k，…，Ｎレイヤモジュール61_Nからなる複数のレイヤモジュールから構成されている。ここで、Ｎは任意の整数であり、ｋは１～Ｎの間の任意の整数である。

【００３７】１レイヤモジュール61_1は、読み込まれたコンフィグレーションファイルの内容に応じて、１レイヤフィルタ61_{1A}および１レイヤ再構築部61_{1B}が構成される。ｋレイヤモジュール61_kは、読み込まれたコンフィグレーションファイルの内容に応じて、ｋレイヤフィルタ61_{kA}およびｋレイヤ再構築部61_{kB}が構成される。Ｎレイヤモジュール61_Nは、読み込まれたコンフィグレーションファイルの内容に応じて、Ｎレイヤフィルタ61_{NA}およびＮレイヤ再構築部61_{NB}が構成される。そして、各レイヤモジュール61_1，…，61_k，…，61_Nは、１からＮまで順に処理される。

【００３８】制御管理部５６２は、各レイヤモジュール61_1，…，61_k，…，61_Nにおいてデータを作成するデータ作成制御部６２ａと、各レイヤモジュール61_1，…，61_k，…，61_Nにおいてデータの記憶を制御するメモリ制御部６２ｂと、解析データＤＴを出力させるためのアナライザ管理部６２ｃとから構成されている。そして、制御管理部５６２は、１レイヤモジュール61_1，…，ｋレイヤモジュール61_k，…，Ｎレイヤモジュール61_Nをそれぞれ制御及び管理する。

【００３９】データ解析部５７は、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部５６からの解析データＤＴに不正が発生しているか判定して解析結果ＣＤＣを出力するデータ解析工程を実行するものである。

【００４０】このデータ解析部５７には、アプリケーション層セッション単位のデータに不正が有るかを解析するアプリケーションアナライザ５７０が設けられている。そして、このアプリケーションアナライザ５７０は、予め読み込んだコンフィグレーションファイルに記載されている内容に基づいてフィルタリング及び再構築されたデータＤＴに不正がないか否かを解析する。

【００４１】図４に、コンフィグレーションファイルの例を示す。この図４において、コンフィグレーションファイル５００は、データ作成部５６からデータ解析部５７に渡すデータＤＴの指定をするための情報やデータ解析部５７で解析する情報を書き込むことができるようになっており、例えば図４に示すような内容を記載できるようになっている。

【００４２】図５に、解放型システム間相互接続（ＯＳＩ；Open System Interconnection）の７層モデルの例を示す。この図に示す階層化モデル８００は、解放型システムの通信機能を７つに階層化したものであり、物理レイヤ８０１、データリンクレイヤ８０２、ネットワークレイヤ８０３、トランスポートレイヤ８０４、セッションレイヤ８０５、プレゼンテーションレイヤ８０６、アプリケーションレイヤ８０７に階層化されている。

【００４３】物理レイヤ８０１は、ビット伝送に必要な物理的条件や電気的条件が定められている。データリンクレイヤ８０２は、データ伝送誤り制御手順等が定められている。ネットワークレイヤ８０３は、公衆パケット交換等各種通信網を介して両端のシステム間でデータのやりとりを可能とするためのものである。トランスポートレイヤ８０４は、両端のシステムの間で透過的で信頼性の高いデータ転送を行うためのものである。セッションレイヤ８０５は、両端のアプリケーションプロセスでの対話を効率よく行うため、同期をとったり伝送モードの選択、送信権の制御を行うためのものである。プレゼンテーションレイヤ８０６は、両端のアプリケーションプロセスが扱うデータを正確にかつ効率よく転送できるようにデータ形式を制御するためのものである。アプリケーションレイヤ８０７は、ユーザが実行する様々なアプリケーションに応じて、ファイル転送、メッセージ通信処理システム、下層端末、遠隔データベースアクセスなどのアプリケーションサービス要求を実行するためのものである。

【００４４】このように構成されたネットワーク不正解析システム５０の動作を図６～図８に説明する。図６に、同システム５０の動作を説明するためのフローチャートを示す。図７，８に、同システムによって処理されるデータの内容の例を示す。

【００４５】ここで、緩衝帯ネットワーク３のコモンバス５１上を一つの意味有る情報ないしデータを構築する複数のデータパケット、例えば通信データ９０ａ，９０ｂ，９０ｃ，９０ｄが流れているとする。

【００４６】これらの通信データ９０ａ，９０ｂ，９０ｃ，９０ｄは、例えば図７に示すように受信先ＩＤ９１ａ，９１ｂ，９１ｃ，９１ｄと、送信元ＩＤ９２ａ，９２ｂ，９２ｃ，９２ｄと、順番９３ａ，９３ｂ，９３ｃ，９３ｄと、データ９４ａ，９４ｂ，９４ｃ，９４ｄとから構成されている。

【００４７】このコモンバス５１上の伝送される通信データ９０ａは、次のようにして構成されている。すなわち、例えば「I am a cracker. 」というアプリケーションレイヤでのデータ９５は細分化されて（ステップ（Ｓ２１）、「I am」というデータ９４ｂと、「ａc」というデータ９４ｄと、「rac 」というデータ９４ａと、「ker.」というデータ９４ｃとに分割されたデータとなる。そして、さらに細分化されて（Ｓ２２）、ヘッダを付けた通信データ９０ａ，９０ｂ，９０ｃ，９０ｄにされ、これらは図５に示す階層化モデル８００によりネットワーク上を伝送されることになる。緩衝帯ネットワーク３上でのデータ単位は、通信データ９０ａ，９０ｂ，９０ｃ，９０ｄとなる。このデータ単位で、緩衝帯ネットワーク３のコモンバス５１上を伝送されることになる。

【００４８】図６に示すように、ネットワーク不正解析システム５０は、コンフィグレーションファイルを読み込む（Ｓ１１）。これにより、データ作成部５６の１レイヤモジュール61_1の１レイヤフィルタ61_{1A}及び１レイヤ再構築部61_{1B}，…，ｋレイヤモジュール61_kのｋレイヤフィルタ61_{kA}及びｋレイヤ再構築部61_{kB}，…，Ｎレイヤモジュール61_NのＮレイヤフィルタ61_{NA}及びＮレイヤ再構築部61_{NB}には、データ解析部５７に渡すデータやフィルタリング及び再構築すべきデータに関するパラメータが設定される。また、このコンフィグレーションファイルにより、データ解析部５７で解析する内容が設定される。

【００４９】ここで、Ｎの値は、図５に示す階層化モデル８００のどの階層までのデータとして再構築するかにより決定される。本実施形態では、Ｎ＝７としてアプリケーション層セッション単位にまで再構築している。但し、Ｎ＝７に限られず、例えばＮ＝３としてネットワーク層セッション単位にまで再構築するようにもできる。いずれの場合もデータ解析に必要なセッション単位にまで再構築するように設定できる。

【００５０】次に、データ収集部５５は、データ収集制御部５５２の制御下に、コモンバス５１の上を伝送されているパケットＰＴの１パケット（例えば通信データ９０ａ）を取り込み（Ｓ１２）、この１パケットがコンピュータシステムの主記憶装置またはハードディスクドライブ装置等にある作業エリアにコピーされる（Ｓ１３）。これにより、この作業エリアにコピーされた１パケットは、階層化モジュール５６１の１レイヤモジュール61_1に取り込まれ、コンフィグレーションファイルの情報に応じて１レイヤ目の処理を実行して次の層のレイヤモジュールに渡す（Ｓ１４）。この１レイヤモジュール61_1では、パケットのヘッダ部のさまざまなフィールドの中の値と、コンフィグレーションファイルで指定されたフィルタ通過パラメータとの比較を行い、コンフィグレーションファイルで指定されているデータを選びだす処理を実行したり、通過処理したりする。また、フィルタ通過処理ではデータを変更しない。

【００５１】次いで、１レイヤモジュール61_1の下層の各レイヤモジュールは、上述と同様にコンフィグレーションファイルの内容に応じてそれぞれ処理を実行する。

【００５２】ｋレイヤモジュール61_kの前のモジュールが処理した結果をｋレイヤモジュール61_kが受け取る。

【００５３】ここで、各レイヤモジュール61_1，…，61_k，…，61_Nでは同様の処理が実行されるので、一例としてｋレイヤモジュール61_kについて詳細に説明する。

【００５４】ｋレイヤモジュール61_kは、予め読み込まれたコンフィグレーションファイルの情報に応じて、受け取ったデータをｋレイヤフィルタ61_{kA}に通すのか否か、ｋレイヤ再構築部61_{kB}を動作させるのか否か、あるいは再構築あるいは非再構築のデータをデータ解析部５７に渡すか否かのパラメータが設定されているので、そのパラメータの設定に従って処理を実行する（Ｓ１５）。

【００５５】例えば、コンフィグレーションファイルの情報の指定によって各パラメータが設定されているとすると、ｋレイヤモジュール61_kでは、上層のレイヤモジュールが処理した結果のデータをｋレイヤフィルタ61_{kA}を通過させたのち（Ｓ１５１；ＹＥＳ）、そのデータを再構築する場合には（Ｓ１５２；ＹＥＳ）、バッファを使用して再構築し（Ｓ１５３）、アプリケーション層単位でのデータにまでの再構築が完了しない場合には（Ｓ１５４；ＮＯ）、ｋレイヤモジュール61_kを抜ける。そして、次のパケットを読み込む（Ｓ１２）。

【００５６】また、バッファを使用して再構築し（Ｓ１５３）、再構築が完了した場合（Ｓ１５４；ＹＥＳ）にはｋレイヤ再構築部61_{kB}のバッファにデータが蓄えてられている。この場合あるいはデータを再構築しない場合（Ｓ１５２；ＮＯ）には、再構築したデータをデータ解析部５７に渡すタイミイグになったときに（Ｓ１５５；ＹＥＳ）、ｋレイヤ再構築部61_{kB}のバッファに蓄えていたデータをデータ解析部５７に渡す（Ｓ１５６）。また、データ解析部５７に渡さないタイミングになったところで（Ｓ１５５；ＮＯ）、これより上側の層のレイヤモジュールにデータを渡す。

【００５７】これにより、ｋレイヤモジュール61_kより上層のレイヤモジュールで処理された結果、図８に示

すように再構築されて（Ｓ２３）、分割されたデータとして「rac 」というデータ９４ａがデータ解析部５７に渡る。

【００５８】以上の処理を１パケット毎に繰り返すことにより（Ｓ１３～Ｓ１６）、ネットワーク上でのデータ単位のパケットＰＴは、図８に示すように再構築され（Ｓ２３）、「I am」というデータ９４ｂと、「ａｃ」というデータ９４ｄと、「rac」というデータ９４ａと、「ker.」というデータ９４ｃとに分割されたデータとなる。さらに、再構築されて（Ｓ２４）、「I am a cracker. 」というアプリケーションレイヤでの元のデータ９５にされる。

【００５９】下位の層のレイヤモジュールが上記のようにコンフィグレーションファイルの情報によって各パラメータが設定されているとすると、Ｎレイヤフィルタ６１$_N$にまでデータが渡る。

【００６０】Ｎレイヤフィルタ６１$_N$では、上述と同様にコンフィグレーションファイルの情報により設定されたパラメータで受け取ったデータの処理を行い、解析データＤＴとしてデータ解析部５７に渡す（Ｓ１６）。

【００６１】また、このフローチャートを使用すれば、複数の種類のフィルタを設定することにより複数の種類のクラッキング等の不正アクセスを同時に監視できる。

【００６２】データ解析部５７では、アプリケーションアナライザ５７０が予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部５６からの解析データＤＴに不正が発生しているか判定している。このアプリケーションアナライザ５７０の判定した結果は、例えばディスプレイ上に、図９に示すような画面９００として表示される。

【００６３】ここで、アプリケーションアナライザ５７０は、不正解析処理を次のいずれか一方あるいは双方を採用するようにしている。但し、これらの処理方法に限られないのは勿論である。

【００６４】（ｉ）注目しているプロトコルでどのような操作をすれば、不正が実行可能かを調べておき、その手順をアプリケーションアナライザ５７０用のコンフィグレーションファイルに記述しておき、解析データＤＴとコンフィグレーションファイルに記載された手順を比較して一致すれば、その通信は不正なものであると判断処理を実行する。

【００６５】（ii）セキュリティを確保するために厳重に管理する必要があるファイルやプログラム等をアプリケーションアナライザ５７０用のコンフィグレーションファイルに記載しておき、記載しておいたリソースに変化があった時点で、その通信は不正なものであると判断処理を実行する。

【００６６】上述したネットワーク不正解析システム５０によれば、例えば次のような不正（クラッキング）を防止できる。

【００６７】（１）ＴＣＰプロトコルのシーケンス番号を推測し、偽のセッションを確保し攻撃対象ホストのファイルに不正アクセスすること。

【００６８】（２）ＳＭＴＰプロトコルのＤＥＢＵＧコマンドを使い、攻撃対象ホストのファイルに不正にアクセスすること。

【００６９】（３）ＭＩＭＥを使って攻撃ホストのセキュリティ管理ファイルを書換え、攻撃ホストにパスワード無しでログインできるようにすること。

【００７０】（４）電子メールやニュースを攻撃対象ホストの処理能力を超えて大量に送りつけ、ネットワーク機能を麻痺させること。

【００７１】（５）telnetプロトコルで、root, guest等めぼしいアカウントにアクセスし、パスワードを適当に推測し、ログインを試みること。

【００７２】（６）TFTPプロトコルを用いて、パスワード無しで攻撃対象ホストのファイルにアクセスすること。

【００７３】以上のように構成された本実施形態のネットワーク不正解析システム５０によれば、次のような利点がある。

【００７４】（１）アプリケーション層までのセッションの再構築を行うことができ、不正解析をおこなう者にとってわかり易いデータを取り扱えるようになった。すなわち、ネットワーク上でのパケットでのデータは細分化されているため解析を行うことが困難であるが、本実施形態のネットワーク不正解析システム５０ではアプリケーション層までのセッションの再構築を行っているので解析データを意味有るデータとすることができる。これにより、データ中の不正の有無を容易に判定することができる。しかも、ネットワークでの不正の多くはデータ部分に発生するので、このデータ部分の不正を検出することにより効率の良い不正解析を行うことができる。

【００７５】（２）層毎の完全なモジュール化により、複数の種類のプロトコルを扱えるようになった。すなわち、ネットワークのプロトコルは図５に示す階層化モデル８００のようにモデル化でき、本実施形態のネットワーク不正解析システム５０はコンフィグレーションファイルの設定に基づきこのモデルを利用して不正の解析を実行するので、新たなプロトコルが開発されても、コンフィグレーションファイル及びデータ作成部５６の新たなプロトコルが対応する層を担当する一部のレイヤモジュールのみを変更することにより対応することができる。このため、データ作成部５６を新たに開発されたプロトコルに対応させるためにデータ作成部５６の全体を変更する必要はないので、プロトコル数の増大に容易に対応することができる。

【００７６】（３）データ解析部での不正解析はコンフィグレーションファイルに記述した検知方法に基づいて行われるので、新たな種類の不正の発生をコンフィグレ

ーションファイルの記述を変更するのみでデータ解析部のソフトウェア自体を変更することなく検出することができる。

【００７７】（４）緩衝帯ネットワーク３との組み合わせにより、任意の通信を取り扱えるようになった。例えば、ＬＡＮ１のステーションや外部ネットワーク７が複数ある場合に、任意の送信元と受信先とについて不正解析を行うことができる。

【００７８】（５）緩衝帯ネットワーク３としてホストから独立しているので、ホスト数の増加にも容易に対応できる。

【００７９】なお、上述の実施形態は本発明の好適な実施の一例ではあるがこれに限定されるものではなく本発明の要旨を逸脱しない範囲において種々変形実施可能である。例えば、図１０に示すように、ネットワーク不正解析システム５０に複数のネットワークインターフェースを設けてマルチホーム化することができる。例えば２つのネットワークインターフェースを有して別個のネットワーク４，５に接続されるときは、ＬＡＮ１と外部ネットワーク７との間の通信は必ずネットワーク不正解析システム５０の内部を通過することになる。このため、ネットワーク不正解析システム５０でのパケットの収集を取りこぼし無く行うことができる。これにより、ネットワークでの不正を高精度に検出することができる。

【００８０】また、図１１に示すように、ネットワーク不正解析システム５０をマルチホーム化すると共に、データ解析部５７からデータ収集部５５へ解析結果をフィードバックさせるようにしても良い。なお、図１１では、データ作成部５６及びデータ解析部５７の具体的な図示は省略している。この場合、データ解析部５７の解析結果によってデータ収集部５５の処理が変化される。これにより、解析の結果、不正行為が行われているセッションやホスト等が特定できた場合、その通信についてはネットワーク不正解析システム５０内を通過させないようにデータ収集部５５を制御することができる。したがって、ネットワークでの不正のＬＡＮ１への侵入を防止することができる。

【００８１】さらに、図１２に示すように、データ作成部５６を、層構造のレイヤフィルタ61_{1A}，…，61_{kA}，…，61_{NA}を有するフィルタリング処理部５８と、層構造のレイヤ再構築部61_{1B}，…，61_{kB}，…，61_{NB}を有する再構築処理部５９とを備えたものにすることができる。この場合、データ作成部５６では、フィルタリング処理部５８においてフィルタリング処理をレイヤの数だけ先にまとめて行い、その後、再構築処理部５９において各レイヤについての再構築処理を行う。このため、解析の対象にならないデータがより早く破棄されるため、不必要な再構築処理やメモリ占有が解消され、ネットワーク不正解析システム５０の動作の高速化を図ることができる。

【００８２】また、上述した各実施形態ではネットワーク不正解析システム５０は図示しないコンピュータシステムから構成されるものとしているが、これには限られない。例えば、上述したネットワーク不正解析方法のデータ収集工程とデータ作成工程とデータ解析工程とをコンピュータに実行させるためのプログラムを記録したＣＤ－ＲＯＭやフロッピーディスク等のコンピュータ読み取り可能な記録媒体を使用して汎用コンピュータを作動させることによりネットワーク不正解析システムを実行することもできる。

【００８３】ここでのプログラムは、具体的には、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集工程を実行するデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程を実行するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成手順からの解析データに不正が発生しているか判定するデータ解析工程を実行するデータ解析手順とをコンピュータに実行させるためのものである。

【００８４】また、上述した実施形態ではデータ収集工程とデータ作成工程とデータ解析工程とを汎用コンピュータに実行させているが、これには限られずこれらの工程を専用のコンピュータから成る独立した装置に実行させるようにしても良い。さらに、上述した実施形態では、これらデータ収集工程とデータ作成工程とデータ解析工程とをコンピュータに実行させているが、これには限られずこれらの工程をシーケンス回路に実行させるようにしても良い。いずれの場合も、データ作成工程においてデータ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するので、データ解析工程ではデータとして意味のある再構築後の解析データを解析対象とすることができる。このため、データ部分に発生した不正を容易に判別することができる。

【００８５】

【発明の効果】以上説明したように、請求項１の発明のネットワークにおける不正を解析する方法によると、データ作成工程においてデータ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成して、データ解析工程ではデータとして意味のある再構築後の解析データを解析対象とすること

ができるので、データ部分に発生した不正を容易に判別することができる。

【００８６】特にネットワークにおける不正はデータ部分に発生することが多いので、このデータ部分の解析を行うことが有効であるが、ネットワーク上で伝送されているパケットではデータ部分が細分化されているので、このデータ部分に不正が発生したかを判定するのは困難である。これに対し、本発明では再構築後の意味のあるデータを解析対象としているのでデータ部分に不正が発生したかを容易に判定することができる。

【００８７】また、請求項２記載の発明のネットワークにおける不正解析装置によると、データ作成部においてデータ収集部からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成して、データ解析部ではデータとして意味のある再構築後の解析データを解析対象とすることができるので、データ部分に発生した不正を容易に判別することができる。

【００８８】さらに、請求項３記載の発明の記録媒体によれば、上述のデータ収集手順とデータ作成手順とデータ解析手順とをコンピュータに実行させるためのプログラムを任意のコンピュータに読み取らせて実行させているので、データ作成手順において、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成して、データ解析手順ではデータとして意味のある再構築後の解析データを解析対象とすることができる。このため、データ部分に発生した不正を容易に判別することができる。

【００８９】したがって、請求項１から３のいずれかに記載した発明によれば次のような効果を得ることができる。

【００９０】（１）アプリケーション層等の任意の層までのセッションの再構築を行うことができ、不正解析をおこなう者にとってわかり易いデータを取り扱えるようになった。すなわち、ネットワーク上でのパケットでのデータは細分化されているため解析を行うことが困難であるが、本実施形態のネットワーク不正解析システムではアプリケーション層までのセッションの再構築を行っているので解析データを意味有るデータとすることができる。これにより、データ中の不正の有無を容易に判定することができる。しかも、ネットワークでの不正の多くはデータ部分に発生するので、このデータ部分の不正を検出することにより効率の良い不正解析を行うことができる。

【００９１】（２）層毎の完全なモジュール化により、複数の種類のプロトコルを扱えるようになった。すなわち、ネットワークのプロトコルは図５に示す階層化モデルのようにモデル化でき、データ作成工程若しくはデータ作成部ではコンフィグレーションファイルの設定に基づきこのモデルを利用して解析データを作成するので、新たなプロトコルが開発されても、コンフィグレーションファイル及びデータ作成工程若しくはデータ作成部の新たなプロトコルが対応する層を担当する一部のレイヤモジュールのみを変更することにより対応することができる。このため、データ作成工程若しくはデータ作成部を新たに開発されたプロトコルに対応させるためにデータ作成工程若しくはデータ作成部の全体を変更する必要はないので、プロトコル数の増大に容易に対応することができる。

【００９２】（３）データ解析工程若しくはデータ解析部での不正解析はコンフィグレーションファイルに記述した検知方法に基づいて行われるので、新たな種類の不正の発生をコンフィグレーションファイルの記述を変更するのみでデータ解析工程若しくはデータ作成部のソフトウェア自体を変更することなく検出することができる。

【００９３】（４）緩衝帯ネットワークとの組み合わせにより、任意の通信を取り扱えるようになった。例えば、ＬＡＮのステーションや外部ネットワークが複数ある場合に、任意の送信元と受信先とについて不正解析を行うことができる。

【００９４】（５）緩衝帯ネットワークとしてホストから独立しているので、ホスト数の増加にも容易に対応できる。

【図面の簡単な説明】

【図１】本発明のネットワーク不正解析方法が適用されたネットワーク不正解析システムの実施の形態を示すブロック図である。

【図２】ネットワーク不正解析システムとネットワークとの接続を示すブロック図である。

【図３】ネットワーク不正解析システムの実施の形態の概略を示すブロック図である。

【図４】同実施の形態で使用するコンフィグレーションファイルの例を示す説明図である。

【図５】同実施の形態にプロトコルの階層化の例を説明するための図である。

【図６】同実施の形態の動作を説明するためのフローチャートである。

【図７】同実施の形態の動作を説明するための図である。

【図８】同実施の形態の動作を説明するための図である。

【図９】同実施の形態で処理した結果を示す図である。

【図１０】ネットワーク不正解析システムの他の実施形態を示すブロック図である。

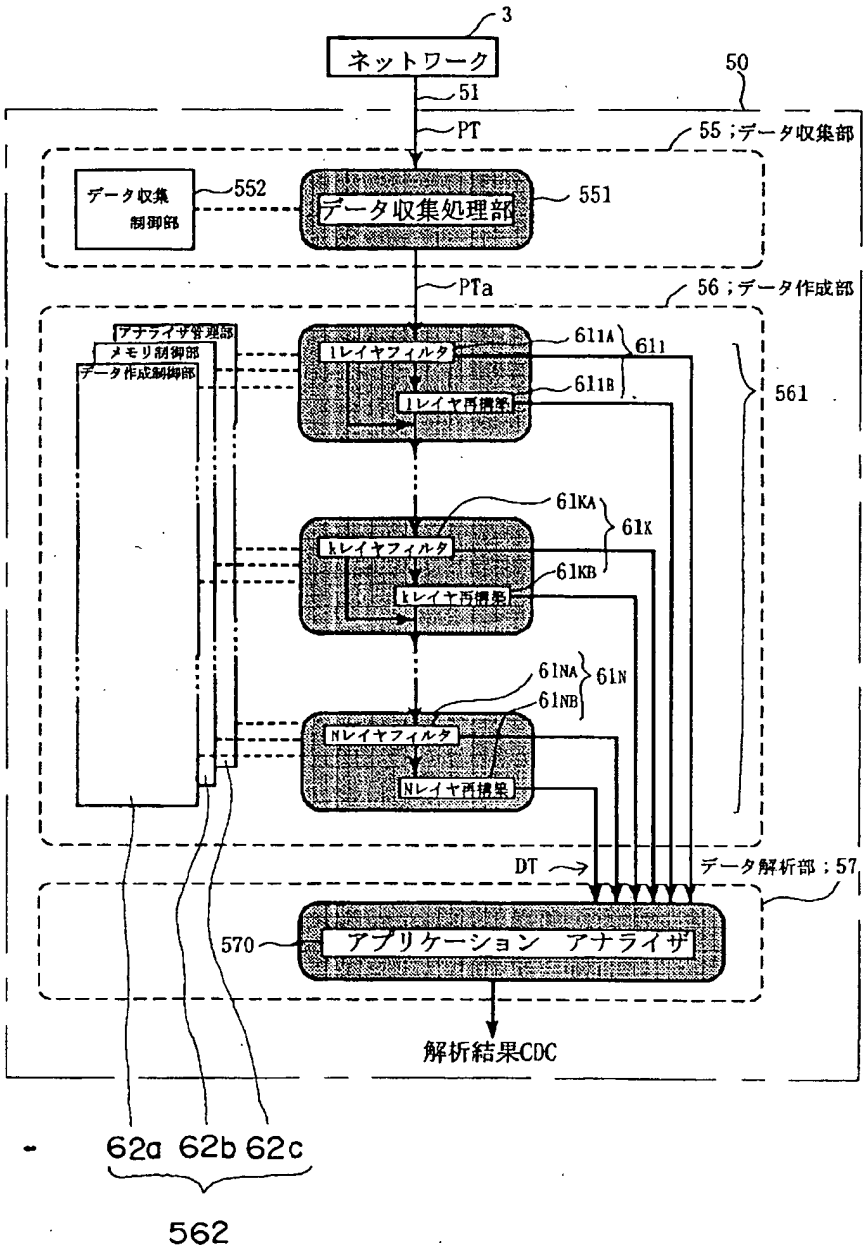
【図１１】ネットワーク不正解析システムの別の実施形態を示すブロック図である。

【図１２】ネットワーク不正解析システムのさらに他の実施形態を示すブロック図である。

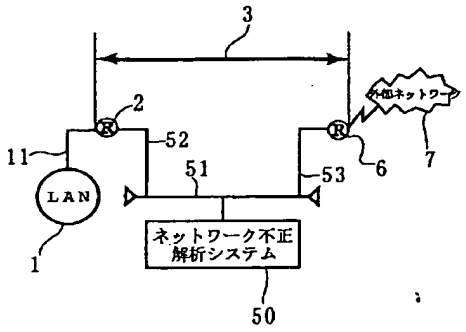
【符号の説明】

1　LAN
3　緩衝帯ネットワーク
7　外部ネットワーク
５０　ネットワーク不正解析システム
５５　データ収集部
５６　データ作成部
５７　データ解析部

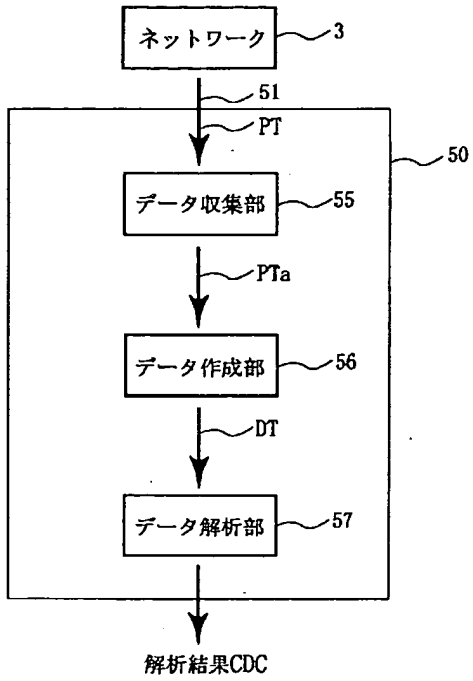
【図１】



【図２】



【図３】

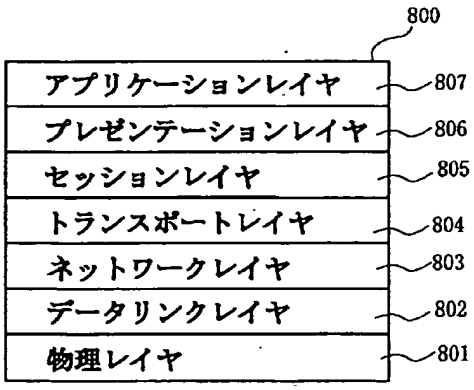


【図４】

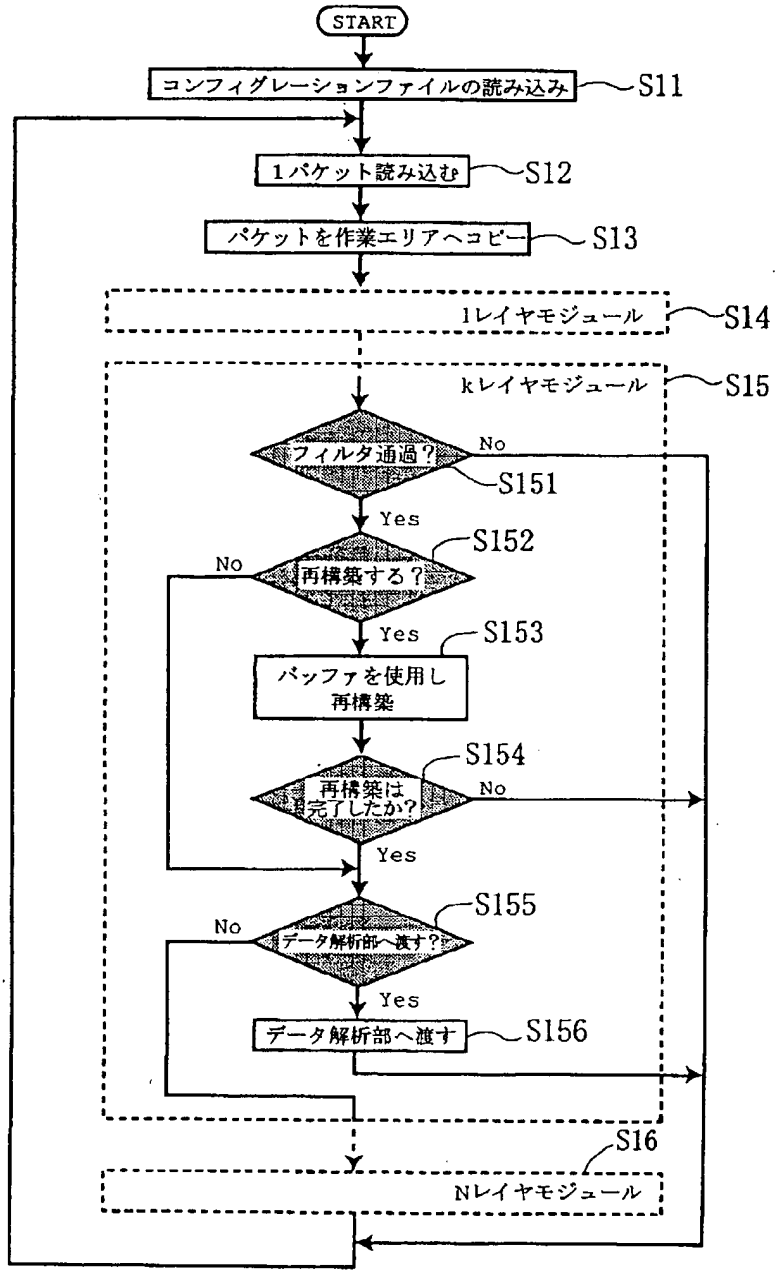
500

```
#-------------------------------------------------------------------#
# Filter for login Analyzer                                         #
#-------------------------------------------------------------------#
filterset {
    physical  = { ether: * <-> aa:bb:cc:xx:yy:zz }
    network   = { ip: * <-> 202.26.95.68 }
    transport = { tcp: * <-> 23 }
    analyzer  = { login-A login.conf -log login.log -dump login.dump}
}
```

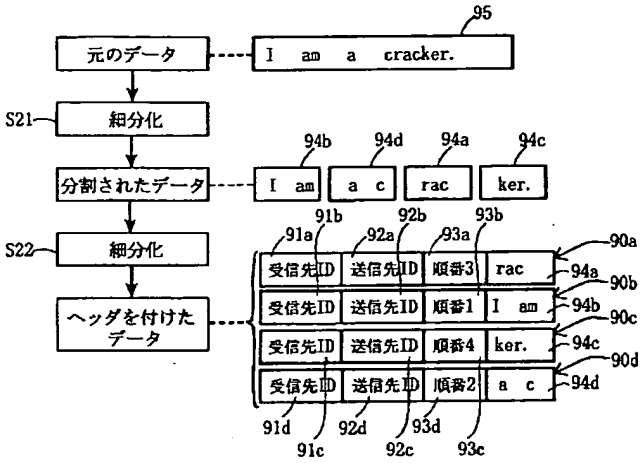
【図５】



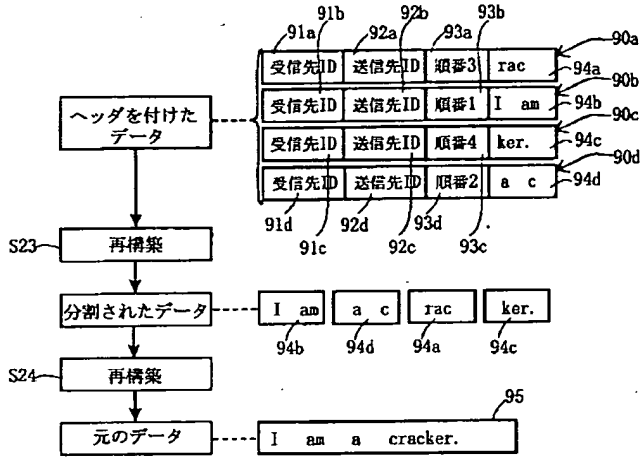
【図６】


START
コンフィグレーションファイルの読み込み
S11
１パケット読み込む
S12
パケットを作業エリアへコピー
S13
1レイヤモジュール
S14
kレイヤモジュール
S15
フィルタ通過？
No
S151
Yes
再構築する？
S152
No
Yes
S153
バッファを使用し
再構築
再構築は
完了したか?
S154
No
Yes
データ解析部へ渡す?
S155
No
Yes
データ解析部へ渡す
S156
S16
Nレイヤモジュール

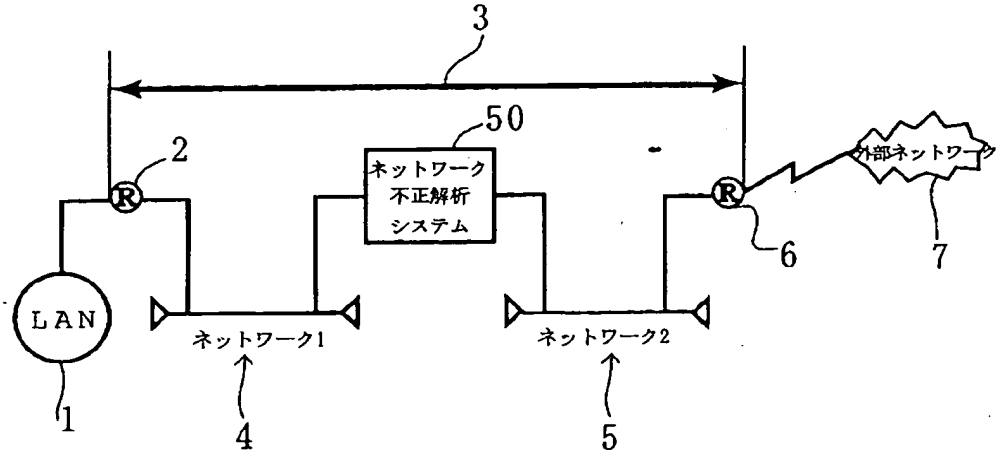
【図７】


元のデータ
I am a cracker.
95
S21
細分化
分割されたデータ
I am
a c
rac
ker.
94b
94d
94a
94c
S22
細分化
ヘッダを付けたデータ
受信先ID
送信先ID
順番3
順番1
順番4
順番2
91a
92a
93a
91b
92b
93b
90a
90b
90c
90d
91c
92c
93c
91d
92d
93d

【図８】


ヘッダを付けたデータ
S23
再構築
分割されたデータ
S24
再構築
元のデータ
I am a cracker.
95
I am
a c
rac
ker.
94b
94d
94a
94c

【図１０】


3
50
2
ネットワーク不正解析システム
外部ネットワーク
LAN
ネットワーク1
ネットワーク2
1
4
5
6
7

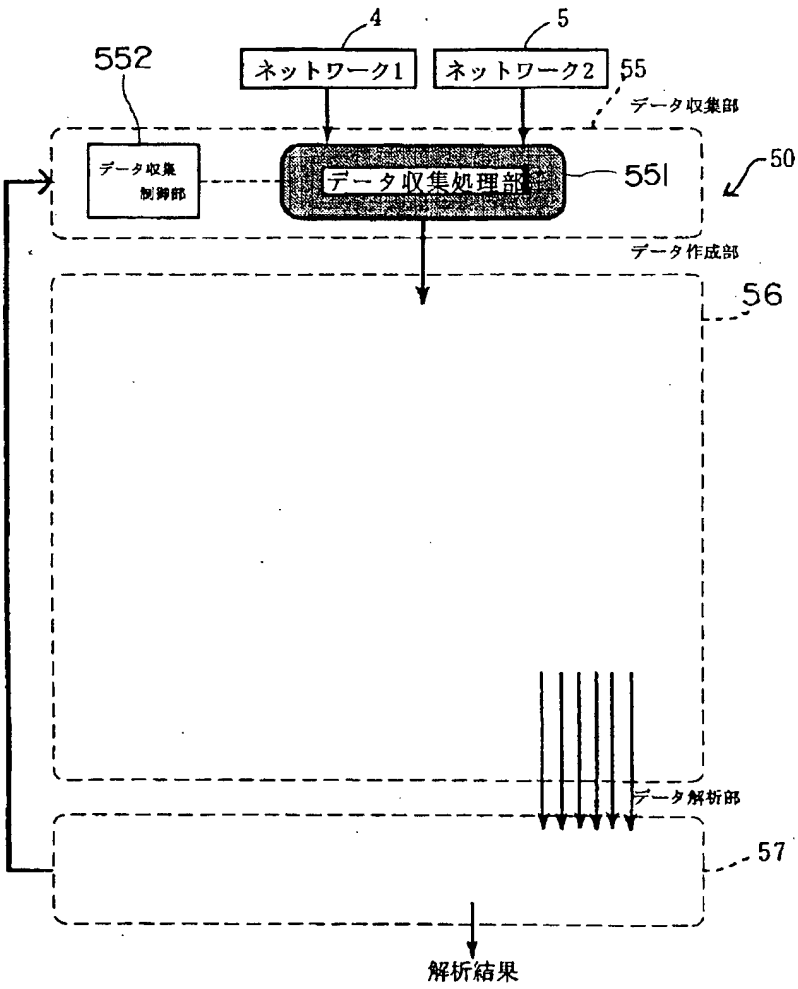
【図９】

900

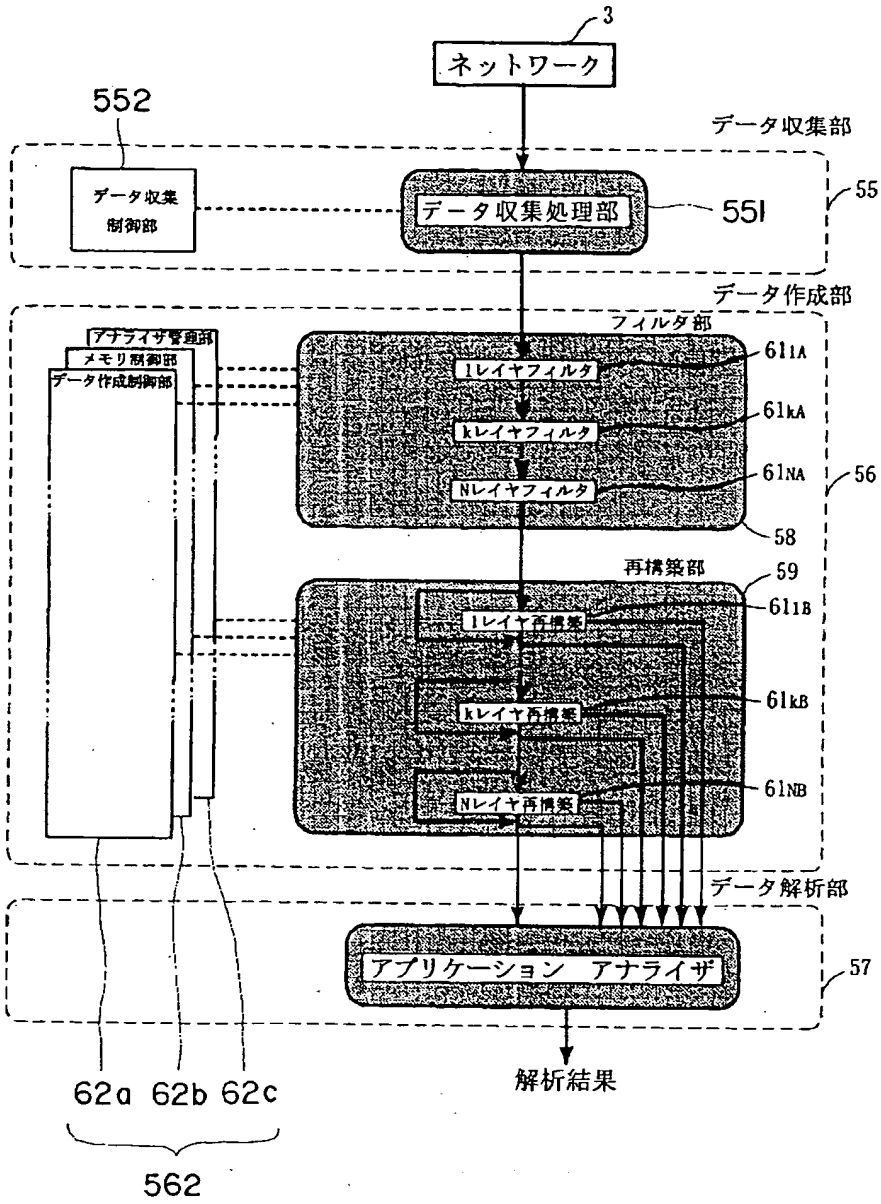
```
-------- Cracking Data contents ------------------------
Date                : Dec 26 13:28:00 1996
Server Address      : 202.26.95.68:23
Client Address      : 202.26.95.69:1024
Defhost Name        : host1
Login Times         : Threshold User = 0  Threshold System = 3
Easy Password Used  : NO

-------- Command Details -------------------------------
S :
S : Welcome to mail.nal.go.jp (ttyp4)
S :
S : login:
C : root
S : Password:
C : rootS
S : Login incorrect
S : login:
C : root
S : Password:
C : root
```

【図１１】



【図１２】


3
ネットワーク
552
データ収集部
データ収集
制御部
データ収集処理部
551
55
データ作成部
アナライザ管理部
メモリ制御部
データ作成制御部
フィルタ部
1レイヤフィルタ
611A
kレイヤフィルタ
61kA
Nレイヤフィルタ
61NA
56
58
再構築部
59
1レイヤ再構築
611B
kレイヤ再構築
61kB
Nレイヤ再構築
61NB
データ解析部
アプリケーション　アナライザ
57
解析結果
62a 62b 62c
562